Notice of Allowability	Application No.	Applicant(s)	
	09/936,570	SORIMACHI ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *7 July 2006 and Interview on 25 September 2006*.

2. ☒ The allowed claim(s) is/are *1-50*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☒ Certified copies of the priority documents have been received in Application No. *09/936,570* .
      3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *9/25/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/27/06

1. In response to amendment filed on 7 July 2006 and Examiner Initiated Interview on 25 September 2006, the amendment to the claims, specification, and drawings are accepted.

2. An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment to amends claims 5, 7, 8, 10, 15, 17, 18, 20, 21, 23, 24-27, 29, 30, 32, and 45-48; was authorized by attorney of record Jason Rhodes in phone interview on 25 September 2006.

Reasons for Allowance

3. Claims 1-50 are allowed over the prior art of record.

The following is a statement of reasons for the indication of allowable subject matter:

In interpreting the claims in light of the specification and applicant's argument, and the Amendment filed 7/7/2006, as well as Examiner's Amendment attached. Examiner finds the claimed invention is patentable distinct from the prior art of record.

The prior arts of record, Markham introducing a system and method for encrypting blocks of plain text, Jakubowski introducing a cryptographic technique that not only provides fast and extremely secure encryption and decryption but also assures integrity of a ciphertext message.

The prior art of record, Markham or Jakubowski fail to anticipate or render Applicant's particular feature that

"interrupting an encryption/decryption process with an encryption/decryption process of another set of continuous data elements" and "that a message

authentication code is generated separately in a generating step while the feedback loop encryption/decryption operation is occurring"

The dependent claims, being further limiting to the independent claims, defined and enabled by the Specification are also allowed.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen. Tran
Patent Examiner
Technology Center 2134
25 September 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/27/06

EXAMINER'S AMENDMENT:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Previously Presented) An encrypting apparatus encrypting first processing data and second processing data comprising:

a memory for storing a status of an encrypting process of a particular processing data,

wherein the encrypting apparatus starts an encrypting process of the second processing data before an encrypting process of the first processing data is completed, thereby interrupting the encryption process of the first processing data between two logically continuous data elements in the first processing data,

the encrypting apparatus causes the memory to store the status of the encrypting process of the first processing data when the encrypting apparatus starts the encrypting process of the second processing data,

the encrypting status of the encrypting apparatus is returned to the status of the encrypting process of the first processing data stored in the memory when the encrypting apparatus restarts encrypting the first processing data, and

the first processing data are a first logically continuous set of data elements, and the second processing data are a second logically continuous set of data elements.

2. (Previously Presented) The encrypting apparatus of claim 1, wherein the encrypting apparatus restarts the encrypting process of the first processing data before the encrypting process of the second processing data is completed,

the memory stores the status of the encrypting process of the second processing data when the encrypting apparatus restarts the encrypting process of the first processing data,

the encrypting status of the encrypting apparatus is returned to the status of the encrypting process of the second processing data stored in the memory when the encrypting apparatus restarts encrypting process of the second processing data.

3. (Previously Presented) The encrypting apparatus of claim 1, wherein the first processing data is a set of consecutive plaintext data blocks and the second processing data is another set of consecutive plaintext data blocks.

4. (Previously Presented) The encrypting apparatus of claim 1, the encrypting apparatus starts encrypting process of the second processing data in response to receiving an interrupt.

5. (Currently Amended) An encrypting apparatus encrypting plaintext data M including plaintext block data M_i (i = 1, 2, 3, ..., I; where I is an integer) and plaintext data N including plaintext block data N_j (j = 1, 2, 3, ..., J; where J is an integer), the encrypting apparatus comprising:

a mechanism for receiving a request to encrypt the plaintext data N during an encrypting process of the plaintext data M;

an encrypting unit for encrypting the plaintext block data M_i to output ciphertext block data C_i(i = 1, 2, 3, ..., I; where I is an integer);

a feedback loop for feeding back the ciphertext block data C_i output from the encrypting unit to the encrypting unit through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving a request to encrypt the plaintext data N and storing the ciphertext block data C_i fed back when the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i so that the encryption process of any of the plaintext block data of the plaintext data N is started; and

a selector for selecting and supplying the ciphertext block data C_i fed back from the feedback line of the feedback loop to the feedback loop in case that the plaintext block data M_{i+1} is encrypted subsequent to the plaintext block data M_i, and for selecting and supplying the ciphertext block data C_i stored in the memory to the feedback loop in case that the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i and the plaintext block data M_{i+1} is encrypted after any of the plaintext block data of the plaintext data N is encrypted,

wherein the plaintext block data M_i (i = 1, 2, 3, ..., I) are logically continuous data elements, and the plaintext block data N_j (j = 1, 2, 3, ..., J) are logically continuous data elements.

6. (Original) The encrypting apparatus of claim 5, wherein the memory includes:

plural registers corresponding to plural pieces of plaintext data; and

a switch for switching the plural registers corresponding to the plaintext data to be encrypted.

7. (Currently Amended) An encrypting method comprising the steps of:

encrypting plaintext block data M_i (i = 1, 2, 3, ..., I; where I is an integer) of first plaintext data M using ciphertext block data C_i (i = 1, 2, 3, ..., I) output from an encrypting module;

storing ciphertext block data C_i to be used for encrypting plaintext block data M_{i+1} of the first plaintext data M in a memory during or after encrypting process of the plaintext block data M_i;

encrypting at least one plaintext block data of second plaintext data N after storing the ciphertext block data C_i to be used for encrypting the plaintext block data M_{i+1} in the memory thereby interrupting the encryption process of the first plaintext data M between M_i and M_{i+1}, wherein M_i and M_{i+1} are two logically continuous data elements in the first processing data; and

encrypting the plaintext block data M_{i+1} of the first plaintext data M by inputting the ciphertext block data C_i to be used for the plaintext block data M_{i+1} stored in the memory and using the encrypting module after encrypting the at least one plaintext block data of the second plaintext data N,

wherein the plaintext block data M_i (i = 1, 2, 3, ..., I) are logically continuous data elements.

8. (Currently Amended) An encrypting apparatus encrypting plaintext data including at least one plaintext block data into ciphertext data using an encrypting unit and generating a message

authentication code (MAC) to ensure an integrity of the ciphertext data, the encrypting apparatus comprising:

an encrypting unit, having a first feedback loop for feeding back ciphertext block data C_i ($i = 1, 2, 3, \ldots$, I; where I is an integer) output by the encrypting unit to the encrypting unit when the plaintext block data M_i ($i = 1, 2, 3, \ldots$, I) is encrypted by the encrypting unit, for inputting the plaintext block data M_i, performing an encrypting process by feeding back the ciphertext block data C_i through the first feedback loop, and outputting the ciphertext block data C_i;

a message authentication code (MAC) generator, having a second feedback loop for feeding back a computed intermediate MAC result, for inputting the ciphertext block data C_i whenever the ciphertext block data C_i is output from the encrypting unit, processing data, feeding back the computed intermediate MAC result by the second feedback loop, and generating the MAC to ensure the integrity of the ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generator before the ciphertext block data C_{i+1} is output from the encrypting unit.

9. (Original) The encrypting apparatus of claim 8,

wherein the encrypting unit and the MAC generator perform alternately the encrypting process and a MAC generating process by sharing one encrypting module and one feedback loop, and

wherein the one feedback loop includes:

a memory for respectively storing and outputting results of the encrypting process and the MAC generating process; and

a selector for selecting alternately the results of the encrypting process and the MAC generating process from the memory to alternately perform the encrypting process and the MAC generating process.

10. (Currently Amended) An encrypting method for encrypting plaintext data including at least one plaintext block data into ciphertext data using an encrypting unit and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the encrypting method comprising:

an encrypting step, including a first feedback step for feeding back ciphertext block data C_i ($i = 1, 2, 3, \ldots$, I; where I is an integer) output from the encrypting unit when the encrypting unit encrypts plaintext block data M_i ($i = 1, 2, 3, \ldots, I$), inputting the plaintext block data M_i, performing an encrypting process by feeding back the ciphertext block data C_i through a first feedback loop, and outputting a ciphertext block data C_i; and

a MAC generating step, including a second feedback step for feeding back a computed intermediate MAC result, inputting the ciphertext block data whenever the ciphertext block data is output from the encrypting step, processing data, feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generating step before the ciphertext block data C_{i+1} is output by the encrypting step.

11. (Previously Presented) A decrypting apparatus decrypting first processing data and second processing data comprising

a memory for storing a status of a decrypting process, wherein

the decrypting apparatus starts the decrypting process of the second processing data before the decrypting process of the first processing data is completed,

the decrypting apparatus causes the memory store the status of the decrypting process of the first processing data when the decrypting process of the second processing data is started, and

the decrypting status of the decrypting apparatus is returned to the status of the decrypting process of the first processing data stored in the memory when the decrypting process of the first processing data is restarted, and

the first processing data comprises a first logically continuous set of data elements when decrypted, and the second processing data comprises a second logically continuous set of data elements when decrypted.

12. (Previously Presented) The decrypting apparatus of claim 11, wherein

the decrypting apparatus restarts the decrypting process of the first processing data before the decrypting process of the second processing data is completed,

the memory stores the decrypting status of the second processing data when the decrypting process of the first processing data is restarted,

the decrypting status of the decrypting apparatus is returned to the decrypting status of the second processing data stored in the memory when the decrypting process of the second processing data is restarted.

13. (Previously Presented) The decrypting apparatus of claim 11, wherein the first processing data is a continuous set of ciphertext data, and the second processing data is another ciphertext data.

14. (Previously Presented) The decrypting apparatus of claim 11, wherein the decrypting apparatus starts the decrypting process of a first block data of the second processing data in response to receiving an interrupt.

15. (Currently Amended) A decrypting apparatus decrypting ciphertext block data C_i (i = 1, 2, 3, ..., I; where I is an integer) included in ciphertext data C and ciphertext block data D_j (j = 1, 2, 3, ..., J; where J is an integer) included in ciphertext data D, the decrypting apparatus comprising:

a mechanism for receiving a request to decrypt the ciphertext data D at an arbitrary timing during a decrypting process of the ciphertext data C;

a decrypting unit for performing the decrypting process of the ciphertext block data C_i to output plaintext block data M_i;

a feedback loop for feeding back the ciphertext block data C_i to be used for decrypting ciphertext block data C_{i+1} to the decrypting unit through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving the request to decrypt the ciphertext data D and storing the ciphertext block data C_i fed back when the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i so that the decrypting process of any of ciphertext block data of the ciphertext data D is started; and

a selector for selecting and supplying the ciphertext block data C_i fed back from the feedback line of the feedback loop in case that the ciphertext block data C_{i+1} is decrypted subsequent to the ciphertext bock data C_i, and for selecting and supplying the ciphertext block data C_i stored in the memory in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i and the ciphertext block data C_{i+1} is decrypted after any of the ciphertext block data of the ciphertext data D is decrypted,

wherein the plaintext block data M_i (i = 1, 2, 3, ..., I) are logically continuous data elements, and decryption of the ciphertext data D results in another plaintext data N being output.

16. (Original) The decrypting apparatus of claim 15, wherein the memory includes:

plural registers corresponding to plural pieces of ciphertext data; and

a switch switching registers corresponding to the ciphertext data to be decrypted.

17. (Currently Amended) A decrypting method comprising steps of:

decrypting ciphertext block data C_i (i = 1, 2, 3, ..., I; where I is an integer) of first ciphertext data C using a decrypting module;

storing ciphertext block data C_i to be used for decrypting ciphertext block data C_{i+1} in a memory ~~during or after decrypting the ciphertext block data C_i~~;

decrypting at least one ciphertext block data of a second ciphertext data D after storing the ciphertext block data C_i to be used for decrypting the ciphertext block data C_{i+1}; and

inputting the ciphertext block data C_i to be used for decrypting the ciphertext block data C_{i+1} stored in the memory after decrypting the at least one ciphertext block data D_j of the ciphertext data D and decrypting the ciphertext block data C_{i+1} of the first ciphertext data C using the decrypting module,

wherein decryption of the ciphertext block data C_i results in a logically-continuous set of plaintext block data M_i (i = 1, 2, 3, ..., I), and decryption of the ciphertext block data D_j results in another plaintext block data N_j being output.

18. (Currently Amended) A decrypting apparatus decrypting ciphertext data including at least one ciphertext block data into plaintext data, and generating a message authentication code (MAC) for ensuring an integrity of the ciphertext data, the decrypting apparatus comprising:

a decrypting unit, including a first feedback loop for feeding back module output block data T_i (i = 1, 2, 3, ..., I; where I is an integer) generated at decrypting data by a decrypting module, for inputting the ciphertext block data C_i (i = 1, 2, 3, ..., I; where I is an integer), decrypting the ciphertext block data C_i using the module output block data T_i fed back through the first feedback loop, and outputting plaintext block data;

a MAC generator, including a second feedback loop for feeding back a computed intermediate MAC result, for inputting ciphertext block data C_i identical to the ciphertext block data C_i input to the decrypting unit, processing the data, outputting the computed intermediate MAC result, feeding back the computed intermediate MAC result through the second feedback loop, and generating the MAC for ensuring the integrity of ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generator before the ciphertext block data C_{i+1} is decrypted by the decrypting unit.

19. (Original) The decrypting apparatus of claim 18,

wherein the decrypting unit and the MAC generator share one decrypting module and one feedback loop and alternately perform a decrypting process and a MAC generating process, and

wherein the one feedback loop includes:

a memory storing and outputting results of the decrypting process and the MAC generating process; and

a selector for alternately selecting the results of the decrypting process and the MAC generating process to output to the decrypting module for alternately performing the decrypting process and the MAC generating process.

20. (Currently Amended) A decrypting method decrypting ciphertext data including at least one ciphertext block data into plaintext data and generating a message authentication code (MAC) for ensuring an integrity of the ciphertext data, the decrypting method comprising:

a decrypting step including a first feedback step for feeding back module output block data T_i ($i = 1, 2, 3, \ldots,$ I; where I is an integer) generated at decrypting data by a decrypting module, inputting the ciphertext block data C_i ($i = 1, 2, 3, \ldots,$ I), decrypting the ciphertext block data C_i using the module output block data T_i fed back through the first feedback step, and outputting plaintext block data;

a MAC generating step including a second feedback step for feeding back a computed intermediate MAC result, inputting ciphertext block data C_i identical to the ciphertext block data C_i input to the decrypting unit, processing the data, outputting the computed intermediate MAC result, feeding back the computed intermediate MAC result by the second feedback step, and generating the MAC for ensuring the integrity of ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generating step before the ciphertext block data C_{i+1} is decrypted by the decrypting step.

21. (Currently Amended) An encrypting apparatus encrypting plaintext data M including plaintext block data M_i (i = 1, 2, 3, ..., I; where I is an integer) and plaintext data N including plaintext block data N_j (j = 1, 2, 3, ..., J; where J is an integer), the encrypting apparatus comprising:

a mechanism for receiving a request to encrypt the plaintext data N during encrypting process of the plaintext data M before completion of the encrypting process of the plaintext data M;

an encrypting module for outputting encrypted data as module output block data T_i;

a feedback loop for feeding back the module output block data T_i output from the encrypting module to the encrypting module through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving the request to encrypt the plaintext data N, and storing the module output block data T_i fed back when the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i so that an encrypting process of any plaintext block data of the plaintext data N is started; and

a selector for selecting and supplying the module output block data T_i fed back through the feedback line of the feed back loop to the feedback loop in case that the plaintext block data M_{i+1} is encrypted subsequent to the plaintext block data M_i, and for selecting and supplying the module output block data T_i stored in the memory to the feedback loop in case that the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i and the plaintext block data M_{i+1} is encrypted after any of plaintext block data of the plaintext data N is encrypted,

wherein the plaintext block data M_i (i = 1, 2, 3, ..., I) are logically continuous data elements, and the plaintext block data N_j (j = 1, 2, 3, ..., J) are logically continuous data elements.

22. (Original) The encrypting apparatus of claim 21, wherein the memory includes:

plural registers corresponding to plural pieces of plaintext data; and

a switch switching registers corresponding to the plaintext data to be encrypted.

23. (Currently Amended) An encrypting method comprising steps of:

encrypting plaintext block data M_i (i = 1, 2, 3, ..., I; where I is an integer) of first plaintext data M using module output block data T_i (i = 1, 2, 3, ..., I) output from an encrypting module;

storing the module output block data T_i to be used for encrypting the plaintext block data M_{i+1} of the first plaintext data M ~~during or after encrypting the plaintext block data M_i~~;

encrypting at least one plaintext block data of second plaintext data N after storing the module output block data T_i to be used for encrypting the plaintext block data M_{i+1}; and

inputting the module output block data T_i to be used for encrypting the plaintext block data M_{i+1} stored in the memory after encrypting the at least one plaintext block data of the second plaintext data N and encrypting the plaintext block data M_i of the first plaintext data M using the encrypting module,

wherein the plaintext block data M_i (i = 1, 2, 3, ..., I) are logically continuous data elements.

24. (Currently Amended) An encrypting apparatus encrypting plaintext data including at least one plaintext block data and generating a message authentication code (MAC) for ensuring an integrity of ciphertext data, the encrypting apparatus comprising:

an encrypting unit, having a first feedback loop for feeding back module output block data T_i (i = 1, 2, 3, ..., I; where I is an integer) output from the encrypting module to the encrypting module when the plaintext block data M_i (i = 1, 2, 3, ..., I) is encrypted by the encrypting unit, for inputting the plaintext data, performing encrypting process by feeding back the module output block data T_i through the first feedback loop, and outputting the ciphertext block data C_i (i = 1, 2, 3, ..., I);

a MAC generator, having a second feedback loop for feeding back a computed intermediate MAC result, for inputting the ciphertext block data C_i whenever the ciphertext block data C_i is output from the encrypting unit, processing data, feeding back the computed intermediate MAC result through the second feedback loop, and generating the MAC to ensure the integrity of the ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generator before the ciphertext block data C_{i+1} is output from the encrypting unit.

25. (Currently Amended) The encrypting apparatus of claim 24,

wherein the encrypting unit and the MAC generator share one encrypting module and one feedback loop to perform alternately the encrypting process and a MAC generating process, and

wherein the one feedback loop includes:

_____a memory for respectively storing and outputting results of the encrypting process and the MAC generating process; and

a selector for selecting alternately the results of the encrypting process and the MAC generating process from the memory to alternately perform the encrypting process and the MAC generating process.

26. (Currently Amended) An encrypting method for encrypting plaintext data including at least one plaintext block data into ciphertext data using an encrypting unit and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data comprising:

an encrypting step, having a first feedback step for feeding back module output block data T_i ($i = 1, 2, 3, \ldots$, I; where I is an integer) output from an encrypting module when the plaintext block data M_i ($i = 1, 2, 3, \ldots$, I) is encrypted, for inputting the plaintext block data, performing an encrypting process by feeding back the module output block data T_i through a first feedback loop, and outputting ciphertext block data C_i ($i = 1, 2, 3, \ldots$, I); and

a MAC generating step, having a second feedback step for feeding back a computed intermediate MAC result, for inputting the ciphertext block data C_i whenever the ciphertext block data C_i is output from the encrypting step, processing data, feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generating step before the ciphertext block data C_{i+1} is output by the encrypting step.

27. (Currently Amended) A decrypting apparatus decrypting ciphertext data C including ciphertext block data C_i (i = 1, 2, 3, ..., I; where I is an integer) and ciphertext data D including ciphertext block data D_j (j = 1, 2, 3, ..., J; where J is an integer), the decrypting apparatus comprising:

a mechanism for receiving a request to decrypt the ciphertext data D during a decrypting process of the ciphertext data C;

a decrypting module for outputting decrypted data as module output block data T_i(i = 1, 2, 3, ..., I; where I is an integer);

a feedback loop for feeding back the module output block data T_i output from the decrypting module to the decrypting module through a feedback line;

a memory, provided in parallel with the feedback line of the feedback loop, for receiving a request to decrypt the ciphertext data D and stores the module output block data T_i fed back in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i

so that the decrypting process of any of the ciphertext block data of the ciphertext data D is started; and

a selector for selecting and supplying the module output block data T_i fed back through the feedback line of the feedback loop to the feedback loop in case that the ciphertext block data C_{i+1} is decrypted subsequent to the ciphertext block data C_i, and for selecting and supplying the module output block data T_i stored in the memory to supply to the feedback loop in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i and the ciphertext block data C_{i+1} is decrypted after any of the ciphertext block data of the ciphertext data D is decrypted,

wherein the plaintext block data M_i (i = 1, 2, 3, ...) are logically continuous data elements, and decryption of the ciphertext data D results in another plaintext data N being output.

28. (Original) The decrypting apparatus of claim 27, wherein the memory includes:

plural registers corresponding to plural ciphertext data; and

a switch for switching the plural registers corresponding to the ciphertext data to be decrypted.

29. (Currently Amended) A decrypting method comprising steps of:

decrypting ciphertext block data C_i (i = 1, 2, 3, ..., I; where I is an integer) of first ciphertext data C using module output block data T_i (i = 1, 2, 3, ..., I) output from a decrypting module;

storing module output block data T_i to be used for decrypting ciphertext block data C_{i+1} of the first ciphertext data C in a memory ~~during or after a decrypting process of the ciphertext block data C_i~~;

decrypting at least one ciphertext block data D_j of second ciphertext data D after storing the module output block data T_i to be used for decrypting the ciphertext block data C_{i+1} in the memory; and

decrypting the ciphertext block data C_{i+1} of the first ciphertext data C using the decrypting module by inputting the module output block data T_i to be used for the ciphertext block data C_{i+1} stored in the memory after decrypting the at least one ciphertext block data of the second ciphertext data D,

wherein decryption of the ciphertext block data C_i results in a logically-continuous set of plaintext block data M_i (i = 1, 2, 3, …, I), and decryption of the ciphertext block data D_j results in another plaintext block data N_j being output.

30. (Currently Amended) A decrypting apparatus decrypting ciphertext data including at least one ciphertext block data into ciphertext data using a decrypting module and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the decrypting apparatus comprising:

a decrypting unit, having a first feedback loop for feeding back ciphertext block data C_i (i = 1, 2, 3, …, I; where I is an integer) output from the decrypting unit to the decrypting unit when the ciphertext block data C_i is decrypted by the decrypting unit, for inputting the ciphertext data,

performing a decrypting process by feeding back the module output block data T_i (i = 1, 2, 3, ..., I) through the first feedback loop, and outputting the ciphertext block data C_i;

a message authentication code (MAC) generator having a second feedback loop for feeding back a computed intermediate MAC result, for inputting the ciphertext block data C_i identical to the ciphertext block data C_i input to the decrypting unit, processing data, feeding back the computed intermediate MAC result through the second feedback loop, and generating the MAC to ensure the integrity of the ciphertext data,

wherein the ciphertext block data C_i is input to the MAC generator before the ciphertext block data C_{i+1} is output by the decrypting unit.

31. (Original) The decrypting apparatus of claim 30,

wherein the decrypting unit and the MAC generator share one decrypting module and one feedback loop to perform alternately the decrypting process and a MAC generating process, and

wherein the one feedback loop includes:

a memory for respectively storing and outputting results of the decrypting process and the MAC generating process; and

a selector for selecting alternately the results of the decrypting process and the MAC generating process from the memory to alternately perform the decrypting process and the MAC generating process.

32. (Currently Amended) A decrypting method for decrypting ciphertext data including at least one ciphertext block data into plaintext data using a decrypting unit and generating a message

authentication code (MAC) to ensure an integrity of the ciphertext data, the decrypting method comprising:

a decrypting step, having a first feedback step for feeding back ciphertext block data C_i (i = 1, 2, 3, ..., I; where I is an integer), for inputting the ciphertext block data C_i, performing a decrypting process of the ciphertext block data C_i fed back through the first feedback step, and outputting plaintext block data; and

a MAC generating step, having a second feedback step for feeding back a computed intermediate MAC result, for inputting the ciphertext block data C_i identical to the ciphertext block data C_i input to the decrypting step, processing data to output the computed intermediate MAC result, feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data, wherein

the ciphertext block data C_i is input to the MAC generating step before the ciphertext block data C_{i+1} is output by the decrypting step..

33. (Original) A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 7.

34. (Original) A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 10.

35. (Original) A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 17.

36. (Original) A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 20.

37. (Original) A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 23.

38. (Original) A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 26.

39. (Original) A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 29.

40. (Original) A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 32.

41. (Original) The encrypting apparatus of claim 1, wherein the encrypting process is performed using block cipher algorithm.

42. (Original) The decrypting apparatus of claim 11, wherein the decrypting process is performed using block cipher algorithm.

43. (Original) The encrypting apparatus of claim 1, wherein the memory stores an intermediate encrypting result of the first processing data and an encryption key to be used for encrypting the first processing data as the status of the encrypting process.

44. (Original) The decrypting apparatus of claim 11, wherein the memory stores an intermediate decrypting result of the second processing data and an encryption key to be used for decrypting the second processing data as the status of the decrypting process.

45. (Currently Amended) An encrypting apparatus comprising:

an encrypting unit with a feedback loop, the encrypting unit being adapted for inputting blocks of plaintext data and outputting ciphertext data, each block of ciphertext data being generated by encrypting a corresponding block of the plaintext data according to a feedback-based scheme; and

a message authentication code (MAC) generator with a second feedback loop, the MAC generator being adapted for inputting each block of ciphertext data output from the encrypting unit and generating a MAC according to a feedback-based scheme for ensuring an integrity of the ciphertext data, and

wherein the MAC generator starts generating the MAC before the blocks of plaintext data have been encrypted by the encrypting unit.

46. (Currently Amended) A decrypting apparatus comprising:

a decrypting unit with a feedback loop, the decrypting unit being adapted for inputting blocks of ciphertext data to decrypt and outputting plaintext data, each block of plaintext data being generated by decrypting a corresponding block of ciphertext data according to a feedback-based scheme; and

a message authentication code (MAC) generator with a second feedback loop, the MAC generator being adapted for inputting each block of plaintext data output from the decrypting unit and generating a MAC according to a feedback-based scheme for ensuring an integrity of the ciphertext data, and

wherein the MAC generator starts generating the MAC before the blocks of ciphertext data have been decrypted by the decrypting unit.

47. (Currently Amended) An encrypting method comprising:

~~an~~ a feedback-based encrypting step for inputting blocks of plaintext data and outputting ciphertext data, each block of ciphertext data being generated by encrypting a corresponding block of the plaintext data according to a feedback-based scheme; and

a feedback-based MAC generating step for inputting each block of ciphertext data output from the encrypting step and generating a MAC according to a second feedback-based scheme for ensuring an integrity of the ciphertext data, and

wherein the MAC generating step starts generating the MAC before the blocks of plaintext data have been encrypted by the encrypting step.

48. (Currently Amended) A decrypting method comprising:

a feedback-based decrypting step for inputting blocks of ciphertext data to decrypt and outputting plaintext data, each block of plaintext data being generated by decrypting a corresponding block of ciphertext data according to a feedback-based scheme; and

a feedback-based MAC generating step for inputting each block of plaintext data output from the decrypting step and generating a MAC according to a second feedback-based scheme for ensuring an integrity of the ciphertext data, and

wherein the MAC generating step starts generating the MAC before the blocks of ciphertext data have been decrypted by the decrypting step.

49. (Original) A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 47.

50. (Original) A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 48.